Приложение № 5

УТВЕРЖДЕНО

приказом директора КГОБУ
«Коррекционная школа-интернат
VI вида»
от 09.01.2018 г. № 01-ОД

ПРАВИЛА
использования средств криптографической защиты информации и электронной подписи в краевом государственном общеобразовательном бюджетном учреждении «Специальная (коррекционная) общеобразовательная школа-интернат VI вида»

г. Владивосток
2018 год

1. Общие положения

1.1. Правила использования средств криптографической защиты информации и электронной подписи разработаны в соответствии с Приказом ФАПСИ от 13.06.2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, в настоящей Инструкции именуется – конфиденциальная информация.

Средства криптографической защиты информации (СКЗИ) и электронной подписи (ЭП) предназначены для подписания электронных документов ЭП с целью подтверждения подлинности информации и её авторства и шифрования этих файлов при передаче по открытым каналам связи для обеспечения конфиденциальности.

2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

Пользователи СКЗИ обязаны:

- не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;
- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего инструктажа.

3. Мероприятия при компрометации криптоключей

Под компрометацией криптоключей в настоящих Правилах понимается хищение, утрата разглашение, несанкционированное копирование и другие

происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать только применяя СКЗИ. Передача по техническим средствам связи криптоключей не допускается.

Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению лицензиата ФАПСИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшиеся (хранящейся) с их использованием конфединциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты.

4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

Требования к обеспечению сохранности конфиденциальной информации в специальных помещениях аналогичны требованиям к помещениям, где выполняются работы, связанные с хранением (обработкой) такой информации. Данная информация содержится в утвержденном «Порядке доступа в помещения, в которых ведется обработка персональных данных в краевом государственном бюджетном учреждении «Специальная (коррекционная) общеобразовательная школа-интернат VI вида.

и скреплено печатью

3 листов

Директор _____ И.Г. Ардашева